AMENDMENTS

In the Claims:

1. (Previously Presented) A method of secure PIN processing in a network transaction between a terminal and a merchant server, wherein the merchant server establishes a network connection between the terminal and a transaction manager, such that the merchant server is not privy to data exchanged between the terminal and the transaction manager, the transaction manager performing the method comprising the steps of:

generating terminal data defining an unshared secret;

generating hardware security module (HSM) data defining an unshared secret;

sending the terminal data to the terminal, wherein the terminal generates corollary data relating to a PIN using the terminal data and user input data, the user input data based on user inputs received by the terminal;

receiving the corollary data from said terminal;

sending the corollary data and the HSM data to a hardware security module, wherein the hardware security module calculates the PIN based on the corollary data and the HSM data, and wherein the hardware security module encrypts the PIN and generates a PIN block that includes the encrypted PIN;

receiving the PIN block from said hardware security module, generating a transaction request including said PIN block and transmitting said transaction request for authentication of the PIN and the transaction;

determining whether a financial institution has authenticated the transaction; and

notifying the merchant server whether the transaction has been authenticated based on the determining step.

2. (Previously Presented) The method of claim 1, wherein said terminal data includes at least one algorithm.

3. (Previously Presented) The method of claim 1, wherein said terminal data includes seed data.

4. (Previously Presented) The method of claim 1, wherein said user input data includes cursor location data.

5. (Previously Presented) The method of claim 1, further comprising the step of receiving transaction data from the terminal and including said transaction data in said transaction request.

6-9. (Cancelled)

10. (Previously Presented) The method of claim 1, wherein said encrypted PIN is encrypted using a split-knowledge key.

11. (Previously Presented) A system for secure PIN processing comprising:

a transaction manager for managing a transaction between a terminal and a merchant server, wherein the transaction manager generates terminal data defining an unshared secret, and wherein the transaction manager generates hardware security module (HSM) data defining an unshared secret;

a transaction module executed by the terminal and communicably connected to said transaction manager for receiving the terminal data from the transaction module, generating corollary data relating to a PIN using the terminal data and user input data, and sending the corollary data to the transaction manager, wherein the merchant server is not privy to data exchanged between the terminal and the transaction manager, wherein the user input data is based on user inputs received by the terminal;

a hardware security module communicably connected to said transaction manager for receiving the corollary data and the HSM data from the transaction manager, calculating the PIN based on the corollary data and the HSM data, encrypting the PIN and generating a PIN block that includes the encrypted PIN; and

wherein said transaction manager receives the PIN block from said hardware security module, generates a transaction request including said PIN block, transmits said transaction request for authentication of the PIN and the transaction, determines whether a financial institution has authenticated the transaction, and notifies the merchant server whether the transaction has been authenticated.

12. (Previously Presented) The system of claim 11, wherein said transaction manager is communicably connected to said transaction module by an open network.

13. (Previously Presented) The system of claim 11, wherein said transaction manager is communicably connected to said hardware security module by a direct connection.

14. (Previously Presented) The system of claim 11 wherein said user input data comprises cursor location data.

15. (Previously Presented) The system of claim 11 wherein said terminal data includes an algorithm.

16. (Previously Presented) The system of claim 11 wherein said HSM data includes an algorithm.

17-20. (Cancelled)